Executive summary

Dell EMC Cyber Recovery protected our test data from a cyber attack

A Dell EMC Cyber Recovery solution with CyberSense can ensure your organization has a path to recovery from destructive cyber attacks

Modern companies can't function without their data. While most organizations realize the importance of backing up critical data in case of hardware failure or natural disaster, many lack adequate protection against attacks from cybercriminals that can similarly threaten financial ruin. The interconnection between company servers, end-user devices, and the rest of the internet at large leaves business-critical data open to attack from malicious entities that take sensitive data hostage, ruining consumer confidence and threatening revenues.

Dell EMC™ Cyber Recovery is a management and automation software solution that exists to protect organizations from these potentially devastating attacks. In the Principled Technologies data center, we set up servers and storage in a Dell EMC Cyber Recovery Vault and launched an attack on our test data. We found that when we infected production files and synced them to the copy in the vault, Index Engines™ CyberSense was able to detect the cyber attack, provide an alert, and report its findings.

With a Dell EMC Cyber Recovery solution, your organization is armed with immutable clean backups waiting in your vault even if cybercriminals manage to infiltrate your production or backup data. This gives you one more line of defense against data and revenue loss while also minimizing costly downtime that could occur without a cyber recovery solution in place.

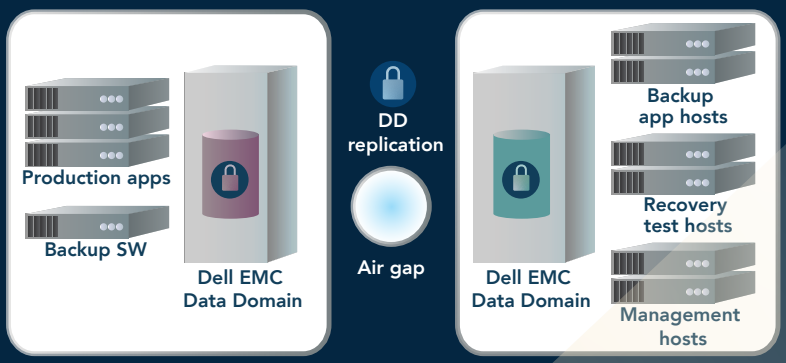
What is Cyber Recovery?

Don't confuse cyber recovery with disaster recovery (DR)—they protect data in different ways, from different kinds of threats. DR involves planning for events that render an organization's primary data center unusable, such as flooding or power grid failure. Cyber recovery solutions exist to enhance an organization by making backup copies more resilient, allowing recovery after more sophisticated attacks.

How the Dell EMC Cyber Recovery Vault works to help you recover from attacks

Dell EMC Cyber Recovery is a complete, isolated recovery solution that can help you minimize downtime, expense, and lost revenue by providing a resilient backup to critical data and a path to recovery from a cyber attack. To start, Dell EMC offers professional services that help you assess, plan, implement, and validate your cyber recovery solution.

Production environments are vulnerable to attack. Dell EMC Cyber Recovery keeps your data in a vault, where it is physically and logically isolated from other systems and locations. Physically, the Cyber Recovery Vault resides in a restricted room or area in your facility accessible only by authorized physical access, which limits the ability of in-house saboteurs that wish to hold your data for ransom to complete their objectives.



CyberSense security analytics looks for indicators of compromised data and can help you discover the who, how, and the why, so you can recover quickly from attack.

Breaking into the vault: Our hands-on tests

To simulate an enterprise solution with real applications running in our data center, we installed and configured a four-node Dell EMC VxRail™ V470F cluster, deploying Microsoft® SQL Server®, clients, and infrastructure VMs. We racked and configured two Data Domain appliances, deployed Networker, and set up backup policies so that the SQL Server databases would back up to a storage pool managed by the first Data Domain appliance.

First, we deployed Index Engines software on a Linux host, added it as an Application Asset in Cyber Recovery, and synced and created a clean backup copy from our production server to our storage in the vault. We ran an Analyze job using CyberSense and found no evidence of attack. When we added files infected with malware to the production server and tried to replicate this data to the vault, CyberSense correctly ascertained that an attack had taken place and raised an alert to Dell EMC Cyber Recovery when it detected the suspicious copy.

While planning for natural disaster or hardware failure with a DR plan is the first step to keeping your data safe, your critical data is still vulnerable without a comprehensive recovery plan that guards against cyber attacks. In our labs, we found that Dell EMC Cyber Recovery offered a recovery solution that provides an isolated immutable copy to analyze what is at risk so organizations can quickly recover critical infrastructure and data assets.

Read the report at http://facts.pt/rkew01n ▶

Principled Technologies®

Facts matter.®